The Secure Brief

RSI NEWSLETTER

ISSUE #2608 | DATE: August 2026

This Month's Brief

August alone touched software supply chain security, AI governance, quantum readiness, PCI DSS, CMMC, cloud security, identity, and vulnerability remediation. Each brings new expectations, tools, assessments, and stakeholders, and the temptation is to meet each one with a separate program, its own spreadsheet, its own owner, its own assessment cycle. That is how compliance quietly becomes unsustainable. The risk was never any single framework; it is the accumulation of parallel work behind all of them.

The better path is structural: map overlapping controls once, reuse evidence where requirements overlap, and assign ownership at the control level rather than by framework.

"The goal isn't to build a new compliance program every time a new requirement appears. It's to build a security and compliance foundation that can absorb change without duplicating the work."

From the RSI Security Desk

Stripe's PCI guidance is a reminder that using a payment provider does not eliminate a merchant's responsibility to validate PCI compliance. The type of validation required, from a self-assessment to an independent assessment, depends on the organization's payment environment and merchant classification.

Read more on Page 3.

Software Supply Chain Security

Know What You're Building With

Microsoft published research on ChainDrop, a self-propagating credential-stealing worm hidden in compromised npm packages. The campaign involved more than 400 compromised packages and spread by republishing malicious updates across the software ecosystem.

Organizations are building more software than ever from open-source components, third-party packages, APIs, and now AI-generated code. Every one of those is a dependency you did not write but still depend on. The takeaway is not that open source is dangerous, it is that software security increasingly rests on understanding not just the code you write, but the components your environment pulls in.

What you can do: Maintain software inventories and SBOMs where appropriate. Review your dependency-management processes. Validate packages before deployment. Monitor for compromised or abandoned dependencies. And build supply-chain security into development workflows rather than bolting it on as a final review.

Source: Microsoft research on ChainDrop.

What Will be

Inside Of The Newsletter

THREAT LANDSCAPE

What Defined August 2026

AI Security Is Moving From Strategy to Implementation

On August 4, Microsoft expanded its Zero Trust for AI strategy with new assessment capabilities, AI-focused checks, implementation guidance, and a new DevSecOps pillar, one that spans 15 control groups and 91 tasks designed to apply Zero Trust principles from source code through cloud deployment.

This is the shift worth watching. The AI conversation is moving past "should we allow AI?" toward "how do we adopt AI while building the right security and governance foundations around it?" Microsoft's update is a clear signal that AI security guidance is becoming operational and specific rather than aspirational, 91 concrete tasks, not a set of principles.

What you can do: Establish a baseline for AI use across the organization. Define ownership for AI systems and agents. Apply least privilege to AI agents and tools. Fold AI systems into your existing identity, data protection, and DevSecOps processes. Start with foundational controls rather than standing up an entirely separate AI security program.

Source: Microsoft Zero Trust for AI update.

AI Is Also Becoming a More Practical Tool for Defenders

The same technology reshaping the threat landscape is increasingly working for defenders. AWS announced new capabilities for its AI-powered Security Agent, including budget controls and finding revalidation for autonomous penetration testing — so teams can retest a specific finding after a fix rather than rerun the entire test, and get a clear status on whether the issue is still exploitable. Microsoft, meanwhile, published a real-world case in which Defender autonomously disrupted a ransomware attack at QNET in 128 seconds.

AI is being applied to work that has always consumed analyst and engineering time: penetration testing, validation, threat modeling, investigation, detection, and response. The point is not that AI replaces security teams. It is that AI can free them from repetitive analysis to spend more time making informed decisions.

Quantum Readiness Is Becoming More Practical

On August 20, Google Cloud announced quantum-safe key import in Cloud KMS, designed to protect sensitive keys in transit and supporting multiple post-quantum cryptographic methods. Google framed it as the first step in the next phase of its post-quantum migration timeline.

That framing matters more than any single feature. Post-quantum preparation is moving off the whiteboard and into the platforms organizations already use. This is not "quantum computers are about to break everything." It is a practical opening to start preparing now — understanding where cryptography lives so future migrations are easier. NIST continues to state that "now is the time to migrate to new post-quantum encryption standards," noting three finalized standards are ready for implementation today.

AWS Security Agent update & Microsoft's 128-second disruption case study

PAYMENT SECURITY

PCI Compliance Still Requires Understanding Scope

The PCI Security Standards Council stayed active through August. A notable FAQ reinforced that SAQ eligibility criteria should not be used on their own to decide which PCI DSS requirements apply, without confirmation from the relevant compliance-accepting entities. The Council also published the first major revision to the PCI Secure Software Standard and its supporting Program Guide.

The recurring misconception is worth naming again: using a payment provider can reduce your PCI scope, but it does not automatically eliminate your PCI responsibility. As Stripe's guidance puts it, PCI compliance is a shared responsibility, and businesses accepting payments must still meet their applicable compliance and validation obligations. August's guidance is a reminder that getting scope and validation right matters just as much as choosing the right technology.

What you can do: Map how payment data enters and moves through your environment. Confirm which systems are actually in scope. Validate the correct SAQ or assessment requirements with the appropriate compliance-accepting entity. Reduce unnecessary handling of cardholder data. Understand exactly where third-party responsibility ends and yours begins.

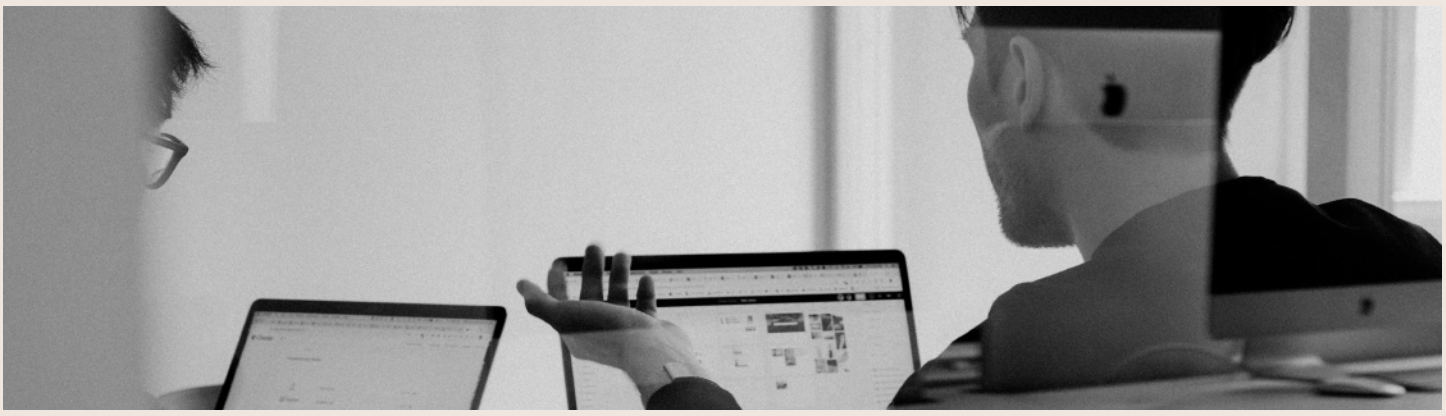
Stripe Guidance & Recent Changes

Stripe's current guidance says that businesses accepting card payments must validate and attest to their PCI DSS compliance, but that does not mean every Stripe customer must undergo a full independent PCI assessment or QSA audit. The validation method depends on the merchant's PCI level, transaction volume, and payment integration.

For many Level 2–4 businesses, that validation is typically a Self-Assessment Questionnaire (SAQ) followed by an Attestation of Compliance. Larger Level 1 merchants may require a more detailed assessment performed by a Qualified Security Assessor (QSA). Stripe says an attestation is generally renewed every 12 months.

Stripe also states that it analyzes a customer's integration method and informs them which PCI validation form to use, and for certain integrations provides assistance completing the SAQ through the Stripe Dashboard.

The accurate takeaway: Stripe is reinforcing PCI validation requirements for businesses using its payment services—not requiring every client to undergo the same full PCI assessment.



Your Compliance Partner

RSI Security is a trusted leader in cybersecurity and compliance, helping organizations of all sizes strengthen defenses, meet regulatory requirements, and maintain resilience in an evolving threat landscape.

Our multidisciplinary team combines deep expertise in threat detection, vulnerability management, regulatory compliance, and incident response to provide complete protection that grows with your business.

From assessment to automation, RSI Security simplifies cybersecurity, empowering your team to focus on what matters most: innovation, growth, and customer trust.

SERVICE HIGHLIGHT

Security That Does Not End at the Assessment

Service Highlight: PCI DSS 4.0.1

This month's spotlight is on the framework that quietly governs anyone who touches cardholder data — and the version now fully in force. PCI DSS 4.0.1 is not a light update. It shifts the standard toward continuous, risk-based security and away from the once-a-year scramble most organizations still run. RSI Security helps you meet it as a direct Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), not a middleman coordinating someone else's assessment.

The hardest part of PCI is rarely the controls themselves. It is scope. Knowing exactly which systems store, process, or transmit cardholder data, and which fall out of scope, determines whether your assessment is manageable or overwhelming. Get scope wrong and everything downstream inflates: more controls, more evidence, more cost. RSI Security's work starts there, mapping how payment data actually moves through your environment so you validate against what matters and nothing you don't.

For teams managing PCI alongside SOC 2, HIPAA, or ISO 27001, the controls overlap more than most realize. Evidence collected once can satisfy requirements across several frameworks, and documentation structured for reuse turns each future assessment into a shorter one. The result is less duplicated work and a compliance program that compounds rather than resets every year.

This is what Partnership Beyond the Assessment means for PCI. Not a report and a door closed, but a direct assessor relationship and the readiness discipline that keeps you compliant between validations — because under 4.0.1, that is where compliance is now measured.

1

Find Payment Data Exposure

Protects cardholder data across every system that stores, processes, or transmits it, reducing the risk of a breach that puts customer payment information in the wrong hands.

2

Reduce Costly Scope Creep

Guards against over-scoped assessments by mapping exactly where payment data lives, so you validate what's in scope and nothing you don't.

3

Combat Compliance Drift

Closes the gaps that open between annual validations, keeping controls and evidence current as your environment changes rather than stale until the next assessment.

4

No Duplicated Audit Effort

Prevents the same evidence being rebuilt framework by framework, reusing PCI controls across SOC 2, HIPAA, and ISO 27001 to cut rework.

SEPTEMBER 2026

Where the Industry Gathers

A lighter month than the August Hacker Summer Camp stretch, but a few relevant gatherings.

Sept 8-10 — **Billington CyberSecurity Summit**
Washington, DC
A leading gathering of government and cybersecurity leaders focused on protecting critical infrastructure, strengthening federal cyber capabilities, and addressing emerging security challenges.

Sept 10 — **FutureCon Charlotte**
Charlotte, NC
FutureCon brings together regional CISOs, security leaders, and technology professionals to discuss current cybersecurity challenges, risk management, and emerging technologies.

Sept 15-16 — **CYBR.SEC.CON**
Houston, TX
CYBR.SEC.CON brings together cybersecurity professionals, industry experts, and technology providers for discussions spanning AI, cloud security, governance, risk, OT, and emerging threats. Its broad range of topics makes it relevant for security leaders managing both technical and compliance priorities.

Sept 22-24 — **National Cyber Summit**
Huntsville, AL
The National Cyber Summit is one of the country's larger cybersecurity events, bringing together government, defense, industry, and academic leaders. With its strong ties to the defense and federal cybersecurity communities, it is particularly relevant for organizations focused on CMMC, NIST 800-171, and government contracting.

> *We strongly support changes that will enhance operational resiliency of the defense industrial base, as well as those that will reduce unnecessary cost, duplicative documentation, inconsistent conformity interpretations, and administrative friction.*
>
> The Cyber AB, Response to the Department of War's "Reforming CMMC and Reducing Compliance Burden" RFI, August 14, 2026

CMMC Is Still Evolving

Build Programs That Can Adapt

The Department of Defense's CMMC Reform RFI closed in August, with the effort explicitly framed around reducing unnecessary burden while improving cybersecurity across the Defense Industrial Base.

The story is no longer just that Phase II was suspended in July — it is that the program is actively being reshaped. That reinforces a point RSI Security has made all year: build security and compliance programs that can adapt, not programs designed only to pass a single assessment. The Department's August messaging asked for input to "cut the red tape and improve the cybersecurity of the DIB." The organizations best positioned for whatever comes next are the ones treating controls as operational, not as a one-time exam.

What you can do: Keep maintaining applicable NIST 800-171 practices. Keep POA&M and remediation processes active. Assign clear control owners. Build repeatable evidence collection. Use the added flexibility to close foundational gaps now, while there is room to do it well.

Source: Department of Defense CMMC updates and Reform RFI.

The Secure Brief

Partnership Beyond the Assessment

RESOURCES

New For Your Organization

1. **Learn More On Our Services.** Check out our list of offered services and how RSI Security can help take your organization to the next level of cyber preparedness.
2. **Cyber Maturity Scorecard.** See where your program stands across people, process, and technology in roughly five minutes.
3. **Weekly Threat Report.** The short-form companion to this monthly brief, tracking the threats that matter as they break.

More Security Data Isn't the Goal — Better Context Is

AWS expanded Security Hub Extended to add Supply Chain Security as its 10th security category, bringing the plan to 23 curated partner solutions with findings aggregated through the Open Cybersecurity Schema Framework. Google Cloud, in an August perspective, emphasized that AI does not eliminate the importance of security fundamentals.

RSI Security helps regulated organizations turn that baseline into a defensible, continuous program, from CMMC and FedRAMP readiness to AI governance and continuous cyber maturity, with advisory continuity that does not end when the assessment does.

YOU HAVE QUESTIONS

Our Team Has Answers

info@rsisecurity.com
Southlake, TX
rsisecurity.com
(858) 252-2448